Splunk analytics for ITSM and CMDB solutions

HIGHLIGHTS

> Provide analytics on your ITSM or CMDB data.

> Correlate IT data with Business data.

> Compare data across environments.

> Monitor availability, performance and compliance.

> Build dashboards for users and managers.

Discover Splunk on

http://www.itconcepts.ch/en/splunk

Whether you use an integrated ITSM solution like BMC Remedy ITSM or only a standalone database for CMDB, you need to provide a lot of services around your solution: usage statistics, availability and performance monitoring, data quality and compliance, and so on. Maybe today these activities are already done by several tools and you would like to consolidate them or you may need to run analysis with external data, this is where ITConcepts can help you with Splunk.

Splunk is a data searching and analyzing tool. No matter where the data is, Splunk can index it in a centralized datastore. Then you can report on that data over time and across sources leading to great correlation capabilities.

Splunk analytics for ITSM solutions reveals your data

IT Operations

Availability: Monitor each component of your ITSM platform from a unique dashboard by centralizing the logs or running some monitoring scripts.

Performance: Monitor the duration of any task to detect too-short- or too-long-running jobs, which may be an issue, or to detect overlapping schedules.

Data quality: Verify the data at each step of the process to detect anomalies. You can detect empty attributes, new or rare values (e.g. incorrect format), missing relationships, etc.

Capacity planning: Follow the evolution of data quantity and build trends. In correlation with the performance monitoring, you can anticipate problems of resources.

Compliance: Compare CI with past states, reference or policy and alert on change of the data.

Licensing: Monitor the number of users by application, the license usage rate by application or the number of connections refused due to lack of license.
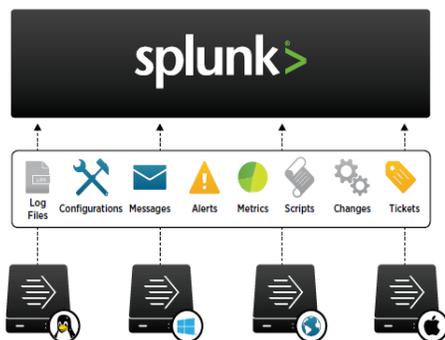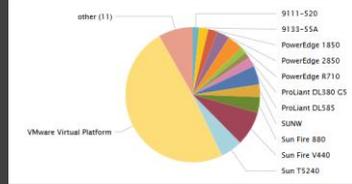
Splunk values
> Easy to install: Install Splunk and get your data within minutes.
> Easy to report on data: Fields and values are automatically extracted and you can report on them using the Pivot function or the search language.
> No database schema to define: You don't need to know the format of the data before indexing it. Splunk indexes data in real time and you can immediately report on it.
> Easy to customize reports: Existing reports (OOTB or your own reports) can be easily duplicated and modified and are immediately available to users.
> Go back in time: Explore your data history for diagnostic or statistics.
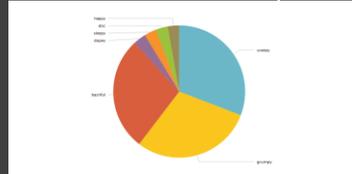> Extend data meaning: Correlate or compare any data from any source.
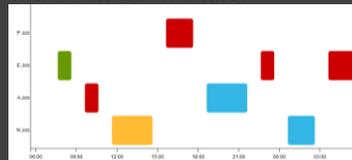
Number of CI by Category over time
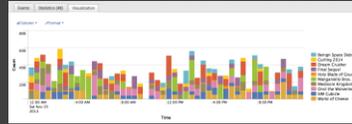
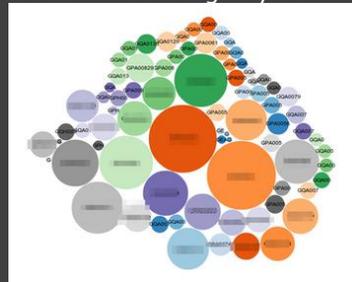**Distribution of server models**

Number of incidents by user

Gantt chart of tasks

List of Incidents by Impact and Resolution time

Number of Change by CI

Performance chart
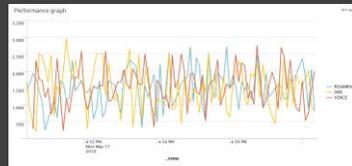
Dashboard

ITSM – CMDB

There are a lot of reports which can be built for each process: list or number of CI with any filter or group, list or number of CI related to another one(s) even across several processes, etc.

Here are some examples:

CMDB: Track the number of CI by Class and Datasets, CI MarkAsDeleted, CI Modified by Users, CI by Category/Type/Item, CI by LastScanDate, List of CI not reconciled (CI (modified) in dataset source and not (modified) in production dataset), etc.

Incident: Track the number of incidents, the resolution times, the delayed incidents, the escalated incidents, the SLA status, the incidents due to changes, the incidents without change, the number of incidents by CI, the services or people impacted by incidents, the number of incidents on the technical infrastructure detected by a user, etc.

Change: Track the number of changes, the number of emergency changes, the time for approval/rejection, the acceptance rate, the realization time, identify unauthorized changes, identify infrastructure or configuration modifications without a change, etc.

Idem for Asset, Problem, Release, Service Request, Service Level, etc.

Business

These examples demonstrate the value of Splunk when you correlate IT and Corporate data:

Business Service Management: Correlate Business Service data with infrastructure monitoring, track the number of service interruptions and their duration, identify service with/without SLA, create User Experience dashboards by application or service.

Correlation with projects: track the number of projects by service, the number of assets by project, the number of incidents or changes by project, the time spent on projects by service, etc.

Correlation with HR: number and technical level of people involved in maintenance by CI, the number of changes or incidents vs. the number of people by CI, the number of training days by user and by CI, etc.

It's now easier to build reports with the new Pivot interface. It opens up the power of Splunk search to non-technical users with an easy-to-use drag and drop interface to explore, manipulate and visualize data.